IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

JOHN STIDWELL, ADAM BROWN, LORI MATA, and MARIA MATA, Individually, and on Behalf of All Others Similarly Situated,	)	**Case No. 1:19-cv-00770**
Plaintiffs,	)	**Honorable John Robert Blakey**
v.	)	
KRONOS, INC., AND NFI INDUSTRIES, INC.	)	
Defendants.	)	

SECOND AMENDED CLASS ACTION COMPLAINT

Plaintiffs John Stidwell, Adam Brown, Lori Mata, and Maria Mata ("Plaintiffs"), by and through counsel, individually and on behalf of all others similarly situated (the "Class") bring the following Second Amended Class Action Complaint pursuant to Rule 23 of the Federal Rules of Civil Procedure against Kronos, Inc., ("Kronos") and NFI Industries, Inc. ("NFI") (collectively, "Defendants"), their subsidiaries and affiliates, to redress and curtail Defendants' unlawful collection, use, storage, and disclosure of Plaintiffs' sensitive biometric data. Plaintiffs allege as follows upon personal knowledge as to themselves, their own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by their attorneys.

NATURE OF THE ACTION

1. Defendant Kronos is a leading provider of human resource management software and services that's best known for helping hundreds of thousands of businesses track employee time and process payroll. In Illinois alone, Kronos provides timekeeping systems to thousands of

employers including Mariano's, Chicago Lakeshore Hospital, Smith Senior Living, Southwest Airlines, Speedway, and Con-Tech Lighting.

2. Defendant NFI is a warehouse and distribution center that provides transit, warehousing, brokerage, and real estate services to clients. NFI has locations throughout the Chicagoland area.

3. When NFI hires an employee, he or she is enrolled in its Kronos employee database. NFI uses the employee database to monitor the time worked by NFI hourly employees.

4. While many employers use conventional methods for tracking time worked (such as ID badge swipes or punch clocks), NFI employees are required to have their fingerprints scanned by a biometric timekeeping device.

5. Biometrics are not relegated to esoteric corners of commerce. Many businesses – such as Defendants' – and financial institutions have incorporated biometric applications into their workplace in the form of biometric timeclocks, and into consumer products, including such ubiquitous consumer products as checking accounts and cell phones.

6. Unlike ID badges or time cards – which can be changed or replaced if stolen or compromised – fingerprints are unique, permanent biometric identifiers associated with each employee. This exposes NFI's employees to serious and irreversible privacy risks. For example, if a database containing fingerprints or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed – like in the recent Yahoo, eBay, Equifax, Uber, Home Depot, MyFitnessPal, Panera, Whole Foods, Chipotle, Omni Hotels & Resorts, Trump Hotels, and Facebook/Cambridge Analytica data breaches or misuses – employees have ***no*** means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

7. In 2015, a data breach at the United States Office of Personnel Management exposed the personal identification information, including biometric data, of over 21.5 million federal employees, contractors, and job applicants. U.S. Off. of Personnel Mgmt., *Cybersecurity Incidents* (2018), *available at* https://www.opm.gov/cybersecurity/cybersecurity-incidents.

8. A black market already exists for biometric data. Hackers and identity thieves have targeted Aadhaar, the largest biometric database in the world, which contains the personal and biometric data – including fingerprints, iris scans, and a facial photograph – of over a billion Indian citizens. *See* Vidhi Doshi, *A Security Breach in India Has Left a Billion People at Risk of Identity Theft*, The Washington Post (Jan. 4, 2018), *available at* https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?utm_term=.b3c70259f138.

9. In January 2018, an Indian newspaper reported that the information housed in Aadhaar was available for purchase for less than $8 and in as little as 10 minutes. Rachna Khaira, *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details*, The Tribune (Jan. 4, 2018), *available at* http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.

10. Recognizing the need to protect its citizens from situations like these, Illinois enacted the Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*, specifically to regulate companies that collect and store Illinois citizens' biometrics, such as fingerprints.

11. Notwithstanding the clear and unequivocal requirements of the law, Defendants disregard NFI employees' statutorily protected privacy rights and unlawfully collect, store, disseminate, and use employees' biometric data in violation of BIPA. Specifically, Defendants have violated and continue to violate BIPA because they did not and continue not to:

A. Properly inform Plaintiff and others similarly situated in writing of the specific purpose and length of time for which their fingerprints were being collected, stored, disseminated and used, as required by BIPA;

B. Provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' fingerprints, as required by BIPA; and

C. Receive a written release from Plaintiff and others similarly situated to collect, store, disseminate or otherwise use their fingerprints, as required by BIPA.

12. Accordingly, Plaintiffs seek an Order: (1) declaring that Defendants' conduct violates BIPA; (2) requiring Defendants to cease the unlawful activities discussed herein; and (3) awarding liquidated damages to Plaintiffs and the proposed class.

PARTIES

13. Plaintiff John Stidwell is a natural person and a citizen of the State of Illinois.

14. Plaintiff Adam Brown is a natural person and a citizen of the State of Illinois.

15. Plaintiff Lori Mata is a natural person and a citizen of the State of Illinois.

16. Plaintiff Maria Mata is a natural person and a citizen of the State of Illinois.

17. Defendant Kronos, Inc. is a corporation organized and existing under the laws of the State of Massachusetts. It is a registered with the Illinois Secretary of State and conducts business in Illinois, including in Cook County.

18. Defendant NFI Industries, Inc., is a corporation existing under the laws of the State of New Jersey, with its principal place of business in Cherry Hill, New Jersey. NFI is registered with the Illinois Secretary of State and conducts business in the State of Illinois, including Cook County.

JURISDICTION AND VENUE

19. This Court has jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2)(A), (d)(5)(B) because the proposed class has 100 or more members, the amount in controversy exceeds $5,000,000.00, and the parties are minimally diverse.

20. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to these claims occurred in this judicial district.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act.

21. Major national corporations started using Chicago and other locations in Illinois in the early 2000s to test "new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS 14/5(c). Given its relative infancy, an overwhelming portion of the public became weary of this then-growing yet unregulated technology. *See* 740 ILCS 14/5.

22. In late 2007, a biometrics company called Pay by Touch, which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions, filed for bankruptcy. The bankruptcy was alarming to the Illinois legislature because there was suddenly a serious risk that millions of fingerprint records – which, similar to other unique biometric identifiers, can be linked to people's sensitive financial and personal data – could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who used the company's fingerprint scanners were completely unaware the scanners were not transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-

bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties.

23. Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information," Illinois enacted BIPA in 2008. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS 14/5.

24. Additionally, to ensure compliance, BIPA provides that, for each violation, the prevailing party may recover $1,000 or actual damages, whichever is greater, for negligent violations and $5,000, or actual damages, whichever is greater, for intentional or reckless violations. 740 ILCS 14/20.

25. BIPA is an informed consent statute which achieves its goal by making it unlawful for a company to, among other things:

> collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first:
>
> 1) informs the subject in writing that a biometric identifier or biometric information is being collected, stored and used;
>
> 2) informs the subject in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> 3) receives a written release executed by the subject of the biometric identifier or biometric information.

See 740 ILCS 14/15(b).

26. BIPA specifically applies to employees who work in the State of Illinois. BIPA defines a "written release" specifically "in the context of employment [as] a release executed by an employee as a condition of employment." 740 ILCS 14/10.

27. Biometric identifiers include retina and iris scans, voiceprints, scans of hand and face geometry, and – most importantly here – fingerprints. *See* 740 ILCS 14/10. Biometric

information is separately defined to include any information based on an individual's biometric identifier that is used to identify an individual. *Id*.

28. BIPA also establishes standards for how companies must handle Illinois citizens' biometric identifiers and biometric information. *See, e.g.*, 740 ILCS 14/15(c)-(d). For example, BIPA prohibits private entities from disclosing a person's biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS 14/15(d)(1).

29. BIPA also prohibits selling, leasing, trading, or otherwise profiting from a person's biometric identifiers or biometric information (740 ILCS 14/15(c)) and requires companies to develop and comply with a written policy – made available to the public – establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting such identifiers or information has been satisfied or within three years of the individual's last interaction with the company, whichever occurs first. 740 ILCS 14/15(a).

30. The Illinois legislature enacted BIPA due to the increasing use of biometric data in financial and security settings, the general public's hesitation to use biometric information, and – most significantly – the unknown ramifications of biometric technology. Biometrics are biologically unique to the individual and, once compromised, an individual is at heightened risk for identity theft and left without any recourse. Biometric data, unlike other personal identifiers such as a social security number, cannot be changed or replaced if hacked or stolen.

31. BIPA provides individuals with a private right of action, protecting their right to privacy regarding their biometrics as well as protecting their rights to know the precise nature for which their biometrics are used and how they are being stored and ultimately destroyed. Unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly

regulates the manner in which entities may collect, store, use, and disseminate biometrics and creates a private right of action for lack of statutory compliance.

II. Defendants Violate the Biometric Information Privacy Act.

32. By the time BIPA passed through the Illinois legislature in mid-2008, most companies who had experimented using employees' biometric data as an authentication method stopped doing so.

33. However, Defendants failed to take note of the shift in Illinois law governing the collection and use of biometric data. As a result, each Defendant continues to collect, store, use, and disseminate Illinois employees' biometric data in violation of BIPA.

34. Specifically, when employees are hired by NFI, they are required to have their fingerprints captured and stored to enroll them in its Kronos employee database(s).

35. NFI uses an employee time tracking system supplied by Kronos that requires employees to use their fingerprint as a means of authentication. Unlike a traditional timeclock, all NFI employees must use their fingerprints to "punch" in and out of work.

36. Upon information and belief, NFI fails to inform its employees that it discloses their fingerprint data to at least one out-of-state third-party vendor, Kronos; fails to inform its employees that it discloses their fingerprint data to other, currently unknown third parties, which host the biometric data in their data centers; fails to inform its employees of the purposes and duration for which it collects their sensitive biometric data; and fails to obtain written releases from employees before collecting their fingerprints.

37. Upon information and belief, Kronos fails to inform NFI employees that it discloses their fingerprint data to other, currently unknown third parties, which host the biometric data in their data centers; fails to inform NFI employees of the purposes and duration for which it collects

their sensitive biometric data; and fails to obtain written releases from employees before collecting their fingerprints.

38. Furthermore, each Defendant fails to provide employees with a written, publicly available policy identifying their retention schedule and guidelines for permanently destroying employees' fingerprints when the initial purpose for collecting or obtaining their fingerprints is no longer relevant, as required by BIPA.

39. In addition, Kronos profits from the use of employees' biometric data. For instance, Kronos markets its biometric time clocks to employers as superior options to traditional time clocks, which can be deceived by "buddy punching" – where one employee punches in to or out of a time clock for another (absent) employee. By marketing its clocks in this manner, Kronos obtains a competitive advantage over other time clock companies and secures profits from its use of biometric data, all while failing to comply with the minimum requirements for handling employees' biometric data established by BIPA.

40. The Pay by Touch bankruptcy, which triggered the passage of BIPA, highlights why such conduct – where individuals are aware that they are providing a fingerprint but are not aware to whom or for what purposes they are doing so – is dangerous. This bankruptcy spurred Illinois citizens and legislators into realizing that it is crucial for individuals to understand when providing biometric identifiers such as a fingerprint, who exactly is collecting their biometric data, where it will be transmitted, for what purposes it will be transmitted, and for how long. Each Defendant disregards these obligations and their employees' statutory rights and instead unlawfully collect, store, use, and disseminate employees' biometric identifiers and information, without ever receiving the individual's informed written consent required by BIPA.

41. Upon information and belief, each Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' biometric data and have not and will not destroy Plaintiff's and other similarly-situated individuals' biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the employee's last interaction with each company.

42. NFI employees are not told what might happen to their biometric data if and when any Defendant merges with another company or worse, if and when each Defendant's business folds, or when the other third parties' that have received their biometric data businesses fold.

43. Since Defendants neither publish BIPA-mandated data retention policies nor disclose the purposes for their collection of biometric data, NFI employees have no idea whether any Defendant sells, discloses, re-discloses, or otherwise disseminates their biometric data. Moreover, Plaintiff and others similarly situated are not told to whom any Defendant currently discloses their biometric data to, or what might happen to their biometric data in the event of a merger or a bankruptcy.

44. These violations have raised a material risk that Plaintiff's and other similarly-situated individuals' biometric data will be unlawfully accessed by third parties.

45. By and through the actions detailed above, Defendants disregarded Plaintiff's and other similarly-situated individuals' legal rights in violation of BIPA.

III. Plaintiffs' Experiences.

46. Plaintiff John Stidwell worked as a Forklift Operator for NFI from November 2016 until October 16, 2018.

47. Plaintiff Adam Brown worked as a dock supervisor for NFI from 2015 to September 2018.

48. Plaintiff Lori Mata worked as a cross dock clerk for NFI from approximately March 2015 until March 2018.

49. Plaintiff Maria Mata worked as a custodian for NFI during 2016.

50. As a condition of employment, each Plaintiff was required to scan his or her fingerprint so NFI could use it as an authentication method to track their time.

51. NFI subsequently stored Plaintiffs' fingerprints in its Kronos database(s).

52. Each Plaintiff was required to scan his or her fingerprint each time he or she began and ended his or her workday.

53. No Plaintiff has ever been informed, prior to the collection of his or her biometric identifiers and/or biometric information, of the specific limited purposes or length of time for which any Defendant collected, stored, used, and/or disseminated his or her biometric data.

54. Prior to the collection of his or her biometric identifiers and/or biometric information, no Plaintiff has ever been informed of any biometric data retention policy developed by any Defendant, nor have they ever been informed whether any Defendant will ever permanently delete their biometric data.

55. Prior to the collection of his or her biometric identifiers and/or biometric information, no Plaintiff has ever been provided with nor ever signed a written release allowing any Defendant to collect, store, use, or disseminate their biometric data.

56. Plaintiffs have continuously and repeatedly been exposed to the risks and harmful conditions created by each Defendant's violations of BIPA as alleged herein.

CLASS ALLEGATIONS

57. Pursuant to Rule 23(a) and 23(b) of the Federal Rules of Civil Procedure, Plaintiffs bring claims on their own behalf and as representatives of all other similarly-situated individuals

pursuant to BIPA, 740 ILCS 14/1 *et seq.*, to recover statutory penalties, prejudgment interest, attorneys' fees and costs, and other damages owed.

58. As discussed *supra*, Section 14/15(b) of BIPA prohibits a company from, among other things, collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's or a customer's biometric identifiers or biometric information, unless it first (1) informs the individual in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the individual in writing of the specific purpose and length of time for which a biometric identifier or biometric information is being collected, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information. 740 ILCS 14/15.

59. Plaintiffs seek class certification under the Illinois Code of Civil Procedure, 735 ILCS 5/2-801 for the following classes of similarly-situated employees under BIPA:

> All individuals working in the State of Illinois who had their fingerprints collected, captured, received, or otherwise obtained or disclosed by any Defendant during the applicable statutory period.

60. This action is properly maintained as a class action under Rule 23 because:

A. The class is so numerous that joinder of all members is impracticable;

B. There are questions of law or fact that are common to the class;

C. The claims of the Plaintiffs are typical of the claims of the class;

D. The Plaintiffs will fairly and adequately protect the interests of the class.

Numerosity

61. The total number of putative class members exceeds 100 individuals. The exact number of class members can easily be determined from NFI's payroll records.

Commonality

62. There is a well-defined commonality of interest in the substantial questions of law and fact concerning and affecting the Class in that Plaintiff and all members of the Class have been harmed by Defendant's failure to comply with BIPA. The common questions of law and fact include, but are not limited to the following:

A. Whether any Defendant collected, captured or otherwise obtained Plaintiffs' biometric identifiers or biometric information;

B. Whether any Defendant properly informed Plaintiffs of its purposes for collecting, using, and storing their biometric identifiers or biometric information;

C. Whether any Defendant obtained a written release (as defined in 740 ILCS 14/10) to collect, use, and store Plaintiffs' biometric identifiers or biometric information;

D. Whether any Defendant disclosed or re-disclosed Plaintiffs' biometric identifiers or biometric information;

E. Whether any Defendant sold, leased, traded, or otherwise profited from Plaintiffs' biometric identifiers or biometric information;

F. Whether any Defendant developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of their last interaction with the individual, whichever occurs first;

G. Whether any Defendant complies with any such written policy (if one exists);

H. Whether any Defendant used Plaintiffs' fingerprints to identify them;

I. Whether any Defendant's violations of BIPA have raised a material risk that Plaintiffs' biometric data will be unlawfully accessed by third parties;

J. Whether the violations of BIPA were committed negligently; and

K. Whether the violations of BIPA were committed recklessly or intentionally.

63. Plaintiffs anticipate that Defendants will raise defenses that are common to the class.

Adequacy

64. Plaintiffs will fairly and adequately protect the interests of all members of the class, and there are no known conflicts of interest between Plaintiffs and class members. Plaintiffs, moreover, has retained experienced counsel who are competent in the prosecution of complex litigation and who have extensive experience acting as class counsel.

Typicality

65. The claims asserted by Plaintiff are typical of the class members she seeks to represent. Plaintiff has the same interests and suffers from the same unlawful practices as the class members.

66. Upon information and belief, there are no other class members who have an interest individually controlling the prosecution of her or her individual claims, especially in light of the relatively small value of each claim and the difficulties involved in bringing individual litigation against one's employer. However, if any such class member should become known, she or she can "opt out" of this action pursuant to Rule 23(b)(3).

Predominance and Superiority

67. The common questions identified above predominate over any individual issues, which will relate solely to the quantum of relief due to individual class members. A class action is superior to other available means for the fair and efficient adjudication of this controversy because individual joinder of the parties is impracticable. Class action treatment will allow a large number of similarly-situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of effort and expense if these

claims were brought individually. Moreover, as the damages suffered by each class member are relatively small in the sense pertinent to class action analysis, the expenses and burden of individual litigation would make it difficult for individual class members to vindicate their claims.

68. Additionally, important public interests will be served by addressing the matter as a class action. The cost to the court system and the public for the adjudication of individual litigation and claims would be substantially more than if claims are treated as a class action. Prosecution of separate actions by individual class members would create a risk of inconsistent and varying adjudications, establish incompatible standards of conduct for Defendants, and/or substantially impair or impede the ability of class members to protect their interests. The issues in this action can be decided by means of common, class-wide proof. In addition, if appropriate, the Court can and is empowered to fashion methods to efficiently manage this action as a class action.

FIRST CAUSE OF ACTION
Violation of BIPA Section 15(a): Failure to Institute, Maintain and Adhere to Publicly-Available Retention Schedule

69. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

70. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention – and, importantly, deletion – policy. Specifically, those companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS 14/15(a).

71. Each Defendant fails to comply with these BIPA mandates.

72. Defendant Kronos is a corporation registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

73. Defendant NFI is a corporation registered to do business in Illinois and thus qualifies as a "private entity" Under BIPA. *See* 740 ILCS 14/10.

74. Plaintiffs are individuals who had their "biometric identifiers" (in the form of their fingerprints) collected by Defendants, as explained in detail in Sections II and III, *supra*. *See* 740 ILCS 14/10.

75. Plaintiffs' biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

76. Each Defendant failed to provide a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA. *See* 740 ILCS 14/15(a).

77. Upon information and belief, each Defendant lacks retention schedules and guidelines for permanently destroying Plaintiffs' and the Class's biometric data and have not and will not destroy Plaintiffs' and the Class's biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with the company.

78. On behalf of themselves and the Class, Plaintiffs seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring each Defendant to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

SECOND CAUSE OF ACTION
Violation of BIPA Section 15(b): Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information

79. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

80. BIPA requires companies to obtain informed written consent from employees before acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject…in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject…in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information…" 740 ILCS 14/15(b) (emphasis added).

81. Each Defendant fails to comply with these BIPA mandates.

82. Defendant Kronos is a corporation registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

83. Defendant NFI is a corporation registered to do business in Illinois and thus qualifies as a "private entity" Under BIPA. *See* 740 ILCS 14/10.

84. Plaintiffs are individuals who had their "biometric identifiers" (in the form of their fingerprints) collected by Defendants, as explained in detail in Sections II and III, *supra*. *See* 740 ILCS 14/10.

85. Plaintiffs' biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

86. Each Defendant systematically and automatically collected, used, stored, and disclosed Plaintiffs' biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

87. Each Defendant did not inform Plaintiffs in writing that their biometric identifiers and/or biometric information were being collected, stored, used, and disseminated, nor did any Defendant inform Plaintiffs in writing of the specific purpose and length of term for which her biometric identifiers and/or biometric information were being collected, stored, used and disseminated as required by 740 ILCS 14/15(b)(1)-(2).

88. By collecting, storing, and using Plaintiffs' and the Class's biometric identifiers and biometric information as described herein, each Defendant violated Plaintiffs' and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq*.

89. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring each Defendant to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

THIRD CAUSE OF ACTION
Violation of BIPA Section 15(d): Disclosure of Biometric Identifiers and Information Before Obtaining Consent

90. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

91. BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS 14/15(d)(1).

92. Each Defendant fails to comply with this BIPA mandate.

93. Defendant Kronos is a corporation registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

94. Defendant NFI is a corporation registered to do business in Illinois and thus qualifies as a "private entity" Under BIPA. *See* 740 ILCS 14/10.

95. Plaintiffs are individuals who had their "biometric identifiers" (in the form of their fingerprints) collected by Defendants, as explained in detail in Sections II and III, *supra*. *See* 740 ILCS 14/10.

96. Plaintiffs' biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

97. Each Defendant systematically and automatically disclosed, redisclosed, or otherwise disseminated Plaintiff's biometric identifiers and/or biometric information without first obtaining the consent required by 740 ILCS 14/15(d)(1).

98. By disclosing, redisclosing, or otherwise disseminating Plaintiffs' and the Class's biometric identifiers and biometric information as described herein, each Defendant violated Plaintiff's and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq*.

99. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring each Defendant to comply with BIPA's requirements for the collection, storage, and use

of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

Wherefore, Plaintiffs respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiffs John Stidwell, Adam Brown, Lori Mata, and Maria Mata as Class Representatives, and appointing Stephan Zouras, LLP, as Class Counsel;

B. Declaring that each Defendant's actions, as set forth above, violate BIPA;

C. Awarding statutory damages of $5,000 for each reckless and/or intentional violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1);

D. Declaring that each Defendant's actions, as set forth above, were reckless or intentional;

E. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class, including an Order requiring Defendants to collect, store, use and disseminate biometric identifiers and/or biometric information in compliance with BIPA;

F. Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3);

G. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable;

H. Provide such further relief as the Court deems just and equitable.

JURY TRIAL

Plaintiffs demand a trial by jury for all issues so triable.

Date: March 18, 2019

Respectfully Submitted,

/s/ Haley R. Jenkins
James B. Zouras
Ryan F. Stephan
Andrew C. Ficzko
Haley R. Jenkins
STEPHAN ZOURAS, LLP
100 N. Riverside Plaza
Suite 2150
Chicago, Illinois 60606
312.233.1550
312.233.1560 *f*
jzouras@stephanzouras.com
rstephan@stephanzouras.com
aficzko@stephanzouras.com
hjenkins@stephanzouras.com

David J. Fish
The Fish Law Firm, P.C.
200 E. 5th Avenue
Suite 123
Naperville, Illinois 60563
630.355.7590
dfish@fishlawfirm.com

ATTORNEYS FOR PLAINTIFFS AND THE PUTATIVE CLASS

CERTIFICATE OF SERVICE

I, the attorney, hereby certify that on March 18, 2019, I electronically filed the attached with the Clerk of the Court using the ECF system which will send such filing to all attorneys of record.

/s/ Haley R. Jenkins